

# On the Optimality of the Golden Code

Frédérique Oggier<sup>1</sup>

Department of Electrical Engineering  
California Institute of Technology  
Pasadena 91125, CA.

Email: frederique@systems.caltech.edu

**Abstract** — In this note, we prove the optimality of the Golden Code inside the class of cyclic algebras based codes. In doing so, we get better insight on these algebraic codes, not only in dimension 2, but more generally for higher dimension, and summarizing the different approaches tried so far to optimize them, we derive design strategies that we believe are the key to either show the optimality of existing codes or give a way to improve them.

## I. INTRODUCTION

We consider the problem of coding for a coherent MIMO channel. The two main design parameters [8] are known to be the rank criterion, which determines the *diversity* of the system, and the minimum determinant, which tells its *coding gain*. In [2, 9, 1], three efficient  $2 \times 2$  codes have been presented independently. In [2],  $2 \times 2$  space-time codes are parameterized using rotation matrices, and through analytical optimization, the code achieving the highest coding gain, among fully diverse and full rate codes, has been found. Note here that full rate means that the 4 coefficients of the  $2 \times 2$  code-word are used to transmit 4 information symbols. In [9], space-time codes were also parameterized using rotation matrices, the goal being this time to find a short length space-time code that achieves the diversity-multiplexing gain (D-MG) tradeoff defined by Zheng and Tse [10]. It was shown in [9] that a minimum determinant lower bounded away from zero was a sufficient condition to reach the tradeoff, thus the parameterized codes were designed to get this condition. Furthermore, optimization of the coding gain of such codes was considered. In [1], an algebraic code has been introduced, based on division algebras [7], called the *Golden Code*, due to the use of the Golden Number. This code was built requiring two special properties: the so-called *non-vanishing determinant*, which appears to be a sufficient condition [9] to achieve the D-MG tradeoff, and a *shaping constraint*, which consists in encoding both the layers of the code applying a unitary matrix on the information symbols vector.

In this note, we prove and discuss the optimality of the Golden Code inside the class of cyclic algebras based codes. The objective is not only the optimality of the code in itself. It is also that among the three approaches

described in [2, 9, 1], only the algebraic approach gives a generalized construction, that can, and has been, extended to higher number of antennas [5]. The purpose is thus, in understanding why the Golden Code is optimal for 2 antennas, to understand what are the general constraints that codes in higher dimensions should satisfy in order to yield optimal codes. In doing so, we also emphasize the energy issues related to the design of such codes, and present the different approaches used so far to construct cyclic algebras based codes.

## II. CYCLIC ALGEBRAS BASED $2 \times 2$ SPACE-TIME CODES

The Golden Code belongs to a family of codes based on cyclic algebras. We recall here how such codes are obtained, but let the reader refer, for example, to [5] for definitions related to cyclic algebras. In the case of two antennas, these algebraic codes are described as follows.

Consider a quadratic field extension of  $\mathbb{Q}(i)$ , that is a set  $L = \{x = a + b\sqrt{d} \mid a, b \in \mathbb{Q}(i)\}$ , denoted by  $L = \mathbb{Q}(i, \sqrt{d})/\mathbb{Q}(i)$ , where  $d$  is (without loss of generality) a *positive* square free integer. Since  $\mathbb{Q}(i) \cap \mathbb{Q}(\sqrt{d}) = \mathbb{Q}$ , the Galois group <sup>2</sup> of  $\mathbb{Q}(i, \sqrt{d})/\mathbb{Q}(i)$  is given by  $\sigma : \sqrt{d} \mapsto -\sqrt{d}$ . Let  $\mathcal{O}_L$  be the ring of integers of  $L$ , and let  $\mathcal{B} = \{1, \nu\}$  denote a  $\mathbb{Z}[i]$ -basis. We consider thus the subset of  $L$  given by  $\mathcal{O}_L = \{x = a + b\nu \mid a, b \in \mathbb{Z}[i]\}$ .

Codewords  $\mathbf{X}$  in a codebook  $\mathcal{C}$ , based on cyclic algebras, are of the form

$$\mathbf{X} = \begin{pmatrix} a + b\nu & c + d\nu \\ \gamma(c + d\sigma(\nu)) & a + b\sigma(\nu) \end{pmatrix}, \quad (1)$$

with  $a, b, c, d \in S = 2^B\text{-QAM} \subset \mathbb{Z}[i]$ , and  $\gamma \in \mathbb{Q}(i)$ .

In the case of the Golden Code, we have  $L = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$ , and  $\nu$  is given by the Golden number, namely,  $\nu = \frac{1+\sqrt{5}}{2}$ . Furthermore,  $\gamma = i$  and the map  $\sigma$  sends  $\sqrt{5}$  to  $-\sqrt{5}$ , in particular,  $\sigma(\nu) = \frac{1-\sqrt{5}}{2}$ .

**Remark 1** Note that this definition is a bit more general than the one given in [5], since here the discriminant of  $\mathbb{Q}(\sqrt{d})$  is not assumed to be coprime with the one of  $\mathbb{Q}(i)$ . One has thus to be careful that  $\mathcal{B} \neq \{1, \sqrt{d}\}$  most of the time, since an integral basis of  $\mathbb{Q}(i, \sqrt{d})/\mathbb{Q}(i)$  is no longer given by the one of  $\mathbb{Q}(\sqrt{d})$ . (Examples will be given in Section III.)

<sup>1</sup>This work was supported by the Swiss National Science Foundation grant PBEL2-110209. and by NSF grant CCR-0133818, by Caltech's Lee Center for Advanced Networking and by a grant from the David and Lucille Packard Foundation.

<sup>2</sup>Roughly,  $L$  is obtained from  $\mathbb{Q}(i)$  by adding  $\theta = \sqrt{d}$ , a root of a polynomial  $p_\theta$ . The Galois group describes mappings among the roots of the polynomial  $p_\theta$ .

## A Diversity and coding gain

In order to ensure good performance, it is known that the codebook has to be fully diverse, and have good coding gain.

Full diversity means that

$$\det(\mathbf{X}_1 - \mathbf{X}_2) \neq 0, \mathbf{X}_1 \neq \mathbf{X}_2 \in \mathcal{C}.$$

If the code is linear, which is the case when using cyclic algebras, the full diversity condition simplifies to

$$\det(\mathbf{X}) \neq 0, \mathbf{0} \neq \mathbf{X} \in \mathcal{C}.$$

Cyclic algebras that yield that condition are called cyclic *division* algebras. This condition is usually not straightforward to check. It has been proven in [1] that the Golden Code is built on a cyclic division algebra.

The coding gain is determined by the *minimum determinant*:

$$\delta_{\min}(\mathcal{C}) = \min_{\mathbf{X} \neq \mathbf{0}} |\det(\mathbf{X})|^2.$$

**Proposition 1** For  $\mathbf{X} \in \mathcal{C}$  and  $\gamma = \frac{\gamma_1}{\gamma_2} \in \mathbb{Q}(i)$ , we have

$$\det(\mathbf{X}) = N_{L/\mathbb{Q}(i)}(a + b\nu) - \gamma N_{L/\mathbb{Q}(i)}(c + d\nu) \in \frac{1}{\gamma_2} \mathbb{Z}[i],$$

so that

$$\delta_{\min}(\mathcal{C}) = \frac{1}{|\gamma_2|^2}.$$

**Proof.** The norm formula is immediate from the definition of norm

$$N_{L/\mathbb{Q}(i)}(x) = x\sigma(x).$$

One way of seeing that the norm falls into  $\mathbb{Z}[i]$  is to notice that it is invariant under  $\sigma$ . Then  $|\det(\mathbf{X})|^2 \in \frac{1}{|\gamma_2|^2} \mathbb{Z}$ , which is at least  $\frac{1}{|\gamma_2|^2}$ . ■

## B Shaping

The notion of efficient shaping has been introduced in [1] as a key property. It means the following: consider the equivalent vectorized channel, where the transmitted signal is denoted by  $\mathbf{x} = (x_1, \dots, x_4)^T$ . While encoding the vector of information symbols  $\mathbf{s} = (s_1, \dots, s_4)^T$  into  $\mathbf{x}$ , the energy has to stay the same. In other words, we want  $\mathbf{x} = \mathbf{U}\mathbf{s}$ , where  $\mathbf{U}$  is unitary. Since points in  $\mathbf{s}$  are discrete, this can be interpreted as looking at a lattice, where  $\mathbf{U}$  is its generator matrix.

One way of getting the shaping is to encode each layer with a unitary matrix, and having  $|\gamma|^2 = 1$ , that is

$$\begin{pmatrix} a + b\nu \\ a + b\sigma(\nu) \end{pmatrix} = \begin{pmatrix} 1 & \nu \\ \sigma(1) & \sigma(\nu) \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

with

$$\begin{pmatrix} 1 & \sigma(1) \\ \nu & \sigma(\nu) \end{pmatrix} \begin{pmatrix} \bar{1} & \bar{\nu} \\ \sigma(1) & \sigma(\nu) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (2)$$

**Remark 2** Note that if  $|\gamma|^2 \neq 1$ , then  $\mathbf{U}$  is not unitary, and one antenna will always need to transmit with more power.

In general such a unitary matrix may not exist. But if it does, one way of finding it is to have  $a, b, c, d$  chosen inside an ideal of  $\mathcal{O}_L$ , of the form  $\mathcal{I} = (\alpha)\mathcal{O}_L$ . Thus  $a = \alpha\tilde{a}, b = \alpha\tilde{b}, c = \alpha\tilde{c}, d = \alpha\tilde{d}$  and

$$\begin{pmatrix} a + b\nu \\ a + b\sigma(\nu) \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{pmatrix} \begin{pmatrix} 1 & \nu \\ 1 & \sigma(\nu) \end{pmatrix} \begin{pmatrix} \tilde{a} \\ \tilde{b} \end{pmatrix}.$$

The codewords of  $\mathcal{C}$  now have the form

$$\mathbf{X} = \begin{pmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{pmatrix} \begin{pmatrix} \tilde{a} + \tilde{b}\nu & \tilde{c} + \tilde{d}\nu \\ \gamma(\tilde{c} + \tilde{d}\sigma(\nu)) & \tilde{a} + \tilde{b}\sigma(\nu) \end{pmatrix}, \quad (3)$$

with  $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in S = 2^B\text{-QAM} \subset \mathbb{Z}[i]$ . Note furthermore that a change of basis from  $\{1, \nu\}$  to a more general basis  $\{\nu_1, \nu_2\}$  may be necessary. This does not change the determinant, and thus, the properties of the code.

**Lemma 1** The minimum determinant of the above code given by (3) is

$$\delta_{\min}(\mathcal{C}) = \frac{|N_{L/\mathbb{Q}(i)}(\alpha)|^2}{|\gamma_2|^2} = \frac{N_{L/\mathbb{Q}}(\alpha)}{|\gamma_2|^2}.$$

**Proof.** This is immediate by computing the determinant of a codeword  $\mathbf{X}$  given in (3). The first matrix has a determinant of  $\alpha\sigma(\alpha) = N_{L/\mathbb{Q}(i)}(\alpha)$  and by Proposition 1, the minimum of the modulus of the second determinant is  $1/|\gamma_2|^2$ . ■

Combining Equations (2) and (3) yield

$$\begin{aligned} 1 &= \det \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \det \left[ \begin{bmatrix} 1 & 1 \\ \nu & \sigma(\nu) \end{bmatrix} \begin{bmatrix} \alpha & 0 \\ 0 & \sigma(\alpha) \end{bmatrix} \begin{bmatrix} \bar{\alpha} & 0 \\ 0 & \sigma(\alpha) \end{bmatrix} \begin{bmatrix} 1 & \bar{\nu} \\ 1 & \sigma(\nu) \end{bmatrix} \right] \\ &= |N_{L/\mathbb{Q}(i)}(\alpha)|^2 \left| \det \begin{pmatrix} 1 & 1 \\ \nu & \sigma(\nu) \end{pmatrix} \right|^2. \end{aligned}$$

Since the relative discriminant  $d_{L/\mathbb{Q}(i)}$  is given by

$$d_{L/\mathbb{Q}(i)} = \det \begin{pmatrix} 1 & 1 \\ \nu & \sigma(\nu) \end{pmatrix}^2,$$

we have proven the following:

**Proposition 2** The minimum determinant is given by

$$\delta_{\min}(\mathcal{C}) = \frac{1}{|\gamma_2 \sqrt{d_{L/\mathbb{Q}(i)}}|^2}.$$

The Golden Code is built over  $\mathbb{Q}(i, \sqrt{5})/\mathbb{Q}(i)$  with  $\gamma = i$ , it has  $d_{L/\mathbb{Q}(i)} = 5$ , thus a minimum determinant of  $1/5$ .

Since the question we address is the optimality of the Golden Code, it can now be expressed in terms of higher coding gain as: if we consider field extensions of  $\mathbb{Q}(i, \sqrt{d})/\mathbb{Q}(i)$ , can we find a smaller discriminant, which furthermore allows to have full diversity?

### III. SMALLER DISCRIMINANTS

The discriminant of the Golden Code is  $d = d_{L/\mathbb{Q}(i)} = 5$ . The goal of this section is to show that number fields with relative discriminant smaller, that is, 4 and 3, do not yield full diversity, while there is no extension of  $\mathbb{Q}(i)$  with relative discriminant 2. One may argue that asking for full diversity for the infinite set of codewords (i.e., asking to have a cyclic division algebra) is too strong, since we finally use only finite signal constellations. This was argued in [6] since a  $4 \times 4$  code built on a nondivision algebra appeared to be very efficient for finite constellations. We will thus show here that actually already 4-QAM symbols do not allow full diversity.

**Remark 3** In this section, we will show that we cannot get a coding better than  $1/5 = 0.2$ , the one of the Golden Code, using cyclic algebras. Note by comparison that the codes proposed in [9] have optimized coding gains of  $(0.2236)^2 = 0.05$  and  $(0.2588)^2 = 0.067$  resp. Codes in [9] also satisfy the shaping constraint, though not stated that way. See Fig. 1 to see the behaviour of the so-called tilted code with coding gain 0.05 compared to the Golden Code.

We first assume that  $\gamma \in \mathbb{Z}[i]$  (i.e.,  $\gamma = i$ ), and discuss the case  $\gamma \in \mathbb{Q}(i)$  at the end of the section.

#### A The case $d = 4$

Consider the field extension  $L = \mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(i)$ , with relative discriminant  $d = 4$ . Its Galois group is given by  $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ . One has to be careful when computing the basis of  $\mathcal{O}_L$  over  $\mathbb{Q}(i)$  (it is not  $\{1, \sqrt{2}\}$  as it would be tempting to think). Denote by  $\zeta_8$  a primitive 8th root of unity. First notice that  $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\zeta_8)$ , since  $\zeta_8 = \frac{\sqrt{2}}{2}(1 + i)$ . Now every element  $x \in \mathcal{O}_L$  can be written

$$x = x_0 + x_1\zeta_8 + x_2\zeta_8^2 + x_3\zeta_8^3 = (x_0 + x_2\zeta_8^2) + \zeta_8(x_1 + x_3\zeta_8^2).$$

A basis is thus given by  $\mathcal{B} = \{1, \zeta_8\}$ . The Galois group can be rewritten as  $\sigma : \zeta_8 \mapsto \zeta_8^5$ . Codewords are of the form

$$\mathbf{X} = \begin{pmatrix} a + b\zeta_8 & c + d\zeta_8 \\ i(c + d\zeta_8^5) & a + b\zeta_8^5 \end{pmatrix},$$

with  $a, b, c, d \in S = 2^B\text{-QAM} \subset \mathbb{Z}[i]$ . Already when sending a 4-QAM constellation, the two following codewords will be transmitted:

$$\mathbf{X}_1 = \begin{pmatrix} (1+i) + b\zeta_8 & c + (1+i)\zeta_8 \\ i[c + (1+i)\zeta_8^5] & (1+i) + b\zeta_8^5 \end{pmatrix}$$

and

$$\mathbf{X}_2 = \begin{pmatrix} (1-i) - b\zeta_8 & -c + (1-i)\zeta_8 \\ i[-c + (1-i)\zeta_8^5] & (1-i) - b\zeta_8^5 \end{pmatrix},$$

where  $b, c$  are any 4-QAM symbols.

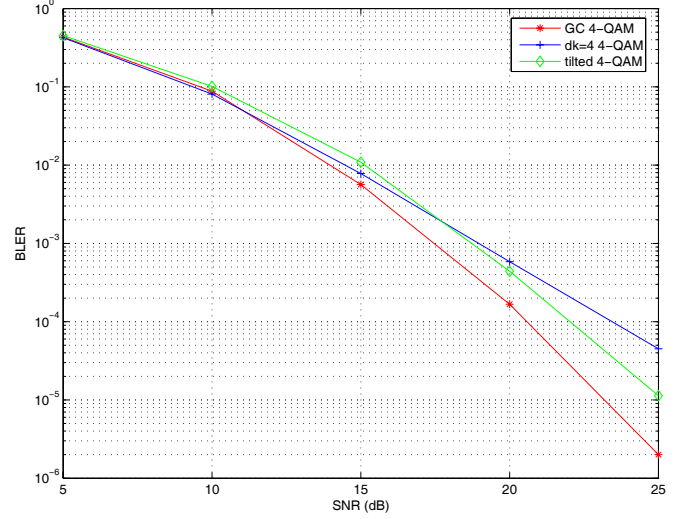


Figure 1: The Golden Code is compared to a non-division algebra based code and to a tilted code.

We have

$$\mathbf{X}_1 - \mathbf{X}_2 = \begin{pmatrix} 2 & 2\zeta_8 \\ i(2\zeta_8^5) & 2 \end{pmatrix},$$

and  $\det(\mathbf{X}_1 - \mathbf{X}_2) = 4(1 - i\zeta_8^6) = 0$ . Thus using the field extension  $L/\mathbb{Q}(i)$  does not give full diversity.

This is illustrated in Fig. 1, where the performance of this code is compared to the Golden Code. The  $x$  axis is the SNR in dBs, and the  $y$  axis the block error rate (BLER). The transmitted constellation is 4-QAM. We notice that at low SNR, the two codes behave similarly, since they have close coding gain ( $1/5$  and  $1/4$  resp.). However, when the SNR increases, there is clearly a loss in diversity for the code based on a non-division cyclic algebra. This loss matches the theory, since using a non-division algebra implies that the code will not be fully diverse. Note that the non-division algebra based code used for the simulation satisfies the shaping constraint.

#### B The case $d = 3$

This case is similar to the previous one. Consider the field extension  $L = \mathbb{Q}(i, \sqrt{3})/\mathbb{Q}(i)$ . The relative discriminant is  $d = 3$ , and the Galois group is given by  $\sqrt{3} \mapsto -\sqrt{3}$ . A basis of  $\mathcal{O}_L$  is given by  $\{1, \frac{\sqrt{3}-i}{2}\}$ .

Again when sending a 4-QAM constellation, the two following codewords will be transmitted:

$$\mathbf{X}_1 = \begin{pmatrix} (1+i) + b\frac{\sqrt{3}-i}{2} & (1+i) + (1+i)\frac{\sqrt{3}-i}{2} \\ i[(1+i) - (1+i)\frac{\sqrt{3}+i}{2}] & (1+i) - b\frac{\sqrt{3}+i}{2} \end{pmatrix}$$

and

$$\mathbf{X}_2 = \begin{pmatrix} (1-i) - b\frac{\sqrt{3}-i}{2} & (1-i) + (1-i)\frac{\sqrt{3}-i}{2} \\ i[(1-i) - (1-i)\frac{\sqrt{3}+i}{2}] & (1-i) + b\frac{\sqrt{3}+i}{2} \end{pmatrix},$$

where  $b$  is any QAM symbols.

We have

$$\mathbf{X}_1 - \mathbf{X}_2 = \begin{pmatrix} 2 & 2 + 2\frac{\sqrt{3}-i}{2} \\ i[2 - 2\frac{\sqrt{3}+i}{2}] & 2 \end{pmatrix},$$

and  $\det(\mathbf{X}_1 - \mathbf{X}_2) = 4(1 - i[(\frac{2-i}{2})^2 - \frac{3}{4}]) = 0$ . Thus using the field extension  $L/\mathbb{Q}(i)$  does not give full diversity.

## C The case $\gamma \in \mathbb{Q}(i)$

Since getting full diversity with  $\gamma \in \mathbb{Z}[i]$  is not easy, in [3], it was suggested to choose  $\gamma \in \mathbb{Q}(i)$ , with  $|\gamma|^2 = 1$ . However, the price to pay in the coding gain is a factor of  $|\gamma_2|^2$ . Since  $\gamma_2 \in \mathbb{Z}[i]$ , we have  $\min |\gamma_2|^2 = 2$  if  $\gamma_2 \neq 1, \pm i$ . Thus even if  $\gamma \in \mathbb{Q}(i)$  may give full diversity, there will be no improvement in the coding gain.

## IV. CODES OVER ORDERS

So far, codewords have been considered with coefficients in  $\mathcal{O}_L$ , or in an ideal of  $\mathcal{O}_L$ . In this section, we investigate codewords with coefficients in an *order* of  $L$ . Before even giving a formal definition, we motivate our approach with an example.

Consider again the scenario of Subsection A, with  $L = \mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(i)$ . Recall that its relative discriminant is  $d = 4$  and its Galois group is given by  $\sigma : \sqrt{2} \mapsto -\sqrt{2}$ . Suppose now that instead of considering the integral basis  $\{1, \zeta_8\}$ , we take  $\mathcal{B} = \{1, \sqrt{2}\}$ . This will generate  $\mathbb{Z}[i][\sqrt{2}] \subset \mathbb{Z}[\zeta_8]$ . As previously, codewords are of the form

$$\mathbf{X} = \begin{pmatrix} a + b\sqrt{2} & c + d\sqrt{2} \\ i(c - d\sqrt{2}) & a - b\sqrt{2} \end{pmatrix},$$

with  $a, b, c, d \in S = 2^B\text{-QAM} \subset \mathbb{Z}[i]$ . The counterexample of Subsection A is no longer valid, and actually, for the 4-QAM constellation, this code gives full diversity. Intuitively, the counterexample was given by  $\zeta_8$ , which does not belong anymore to  $\mathbb{Z}[i][\sqrt{2}]$ .

The set  $\mathbb{Z}[i][\sqrt{2}]$  is called an *order*, and the above example shows that using an order of  $L$  may allow to give full-diversity for constellations for which  $\mathcal{O}_L$  does not.

**Definition 1** An order of  $L$  is a ring in  $L$  that also has a  $\mathbb{Z}$ -basis of  $n$  elements (where  $n$  is the degree of  $L$  over  $\mathbb{Q}$ ).

The ring of integers  $\mathcal{O}_L$  is an order, called the *maximal order* of  $L$ , since it can be shown that all other orders are included in  $\mathcal{O}_L$ .

In Section III, we showed that the Golden Code is optimal in the sense that no other codes built over the ring of integers of number fields with smaller discriminant can be obtained, and thus, because we could not get full diversity. With respect to the example above, we know now that there are codes built over orders that can achieve full diversity when this is not possible with the ring of integers. In order to claim the optimality of the Golden Code,

we have to make sure that none of these codes built over orders can do better. To prove so, we will show that the minimum determinant obtained with these codes cannot do better than the 1/5 of the Golden Code.

Let  $\mathcal{C}$  be a codebook built over an order  $\mathcal{O}$ , with codewords  $\mathbf{X}$  such that

$$\mathbf{X} = \begin{pmatrix} a + b\mu & c + d\mu \\ i(c + d\sigma(\mu)) & a + b\sigma(\mu) \end{pmatrix},$$

with  $a, b, c, d \in S = 2^B\text{-QAM} \subset \mathbb{Z}[i]$ , and  $\{1, \mu\}$  a basis of the order  $\mathcal{O}$ . In order to obtain the shaping constraint, similarly as before, one may consider an ideal of the order.

We first check that the result of Proposition 1 is still valid. We know now that we can restrict to the case where  $\gamma \in \mathbb{Z}[i]$ .

**Lemma 2** If the code is built over an order of  $L$ , then

$$\delta_{\min}(\mathcal{C}) = 1.$$

**Proof.** Since an order is a ring, it contains 1. Thus the matrix identity belongs to the codebook. ■

Let  $\mathcal{I} = (\beta)\mathcal{O}$  be an ideal of  $\mathcal{O}$ . Following the computations to prove Proposition 2, we have that

$$1 = |N_{L/\mathbb{Q}(i)}(\beta)|^2 \left| \det \begin{pmatrix} 1 & 1 \\ \mu & \sigma(\mu) \end{pmatrix} \right|^2,$$

except that this time, we consider the *relative discriminant* of the order  $\mathcal{O}$ :

$$\text{disc}(\mathcal{O}) = \det \begin{pmatrix} 1 & 1 \\ \mu & \sigma(\mu) \end{pmatrix}^2.$$

So what is left is to compare the discriminant of  $\mathcal{O}$  with  $d_{L/\mathbb{Q}(i)}$ .

**Lemma 3** We have

$$|\sqrt{\text{disc}(\mathcal{O})}|^2 = m |\sqrt{d_{L/\mathbb{Q}(i)}}|^2, \quad m \in \mathbb{Z}, \quad m \geq 2.$$

**Proof.** Let  $\{1, \mu\}$  be a basis of  $\mathcal{O}$ , and  $\{1, \nu\}$  be a basis of  $\mathcal{O}_L$ . We have

$$\begin{pmatrix} 1 & 0 \\ w & z \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \nu & \sigma(\nu) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \mu & \sigma(\mu) \end{pmatrix}$$

with  $w, z \in \mathbb{Z}[i]$ . Thus

$$z \sqrt{d_{L/\mathbb{Q}(i)}} = \sqrt{\text{disc}(\mathcal{O})}.$$

The determinant  $z$  cannot be a unit, since  $\mathcal{O}$  is strictly included in  $\mathcal{O}_L$ . Thus  $|z|^2 = m \in \mathbb{Z}$  is at least 2. ■

As an example, consider  $\mathbb{Z}[i][\sqrt{2}] \subset \mathbb{Z}[\zeta_8]$ . We have

$$\begin{pmatrix} 1 & 0 \\ 0 & i-1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \zeta_8 & \zeta_8^5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix},$$

and thus  $(i-1)\sqrt{d_{L/\mathbb{Q}(i)}} = \sqrt{\text{disc}(\mathcal{O})}$ , which gives  $2 \cdot 4 = 8$ .

To summarize, since  $|\text{disc}(\mathcal{O})| \geq 2|d_{L/\mathbb{Q}(i)}|$ , we have

$$\begin{cases} |\text{disc}(\mathcal{O})| \geq 8 \text{ for } \mathbb{Q}(i, \sqrt{2})/\mathbb{Q}(i) \\ |\text{disc}(\mathcal{O})| \geq 6 \text{ for } \mathbb{Q}(i, \sqrt{3})/\mathbb{Q}(i) \end{cases}$$

which completes the proof of optimality of the Golden Code.

To conclude this section, let us note that we have considered codes built over orders of the algebra, but we restricted ourselves to orders coming from orders of  $\mathcal{O}_L$ . There are other orders in the algebra, that do not come from orders of  $\mathcal{O}_L$ , though there is no explicit description for such orders. An attempt has been done [4] to work with such orders. The basis of an order is used to view the order as a lattice. The goal of this work is then to optimize the density of the lattice, while keeping a small determinant. This translates into looking for orders with minimal discriminant. The drawback of this approach is that it does not consider energy constraint. For example, since  $|\gamma|^2 \neq 1$ , one antenna is transmitting with more energy, and the code is unbalanced. Furthermore, the encoding changes the energy of the system. Consequently, the codes in [4] did not improve on the Golden Code.

## V. MORALITY OF THE STORY

The proof of the optimality of the Golden Code shows three main things. The first one is that since the coding gain depends on the discriminant, the goal is to find a number fields with a small discriminant over  $\mathbb{Q}(i)$ . The restriction on number fields with odd discriminant made in [5] is restrictive. Though it allows to compute easily a  $\mathbb{Z}[i]$ -basis, it also prevents to get smaller discriminants. The second point is that the energy issue is critical. Decreasing the minimum determinant without taking into account the energy will not give any gain. Thus, getting an energy efficient encoding with a good choice of  $\gamma$  is crucial. Finally, note that one should consider non maximal orders. Though they induce a loss in the coding gain, they may allow to get an efficient encoding on a number field with very small discriminant, so that all together, there is still an improvement on known constructions.

The summary of what should be done to determine optimal constructions for higher number of antennas is thus: to find number fields with a small discriminant over  $\mathbb{Q}(i)$  (small meaning smaller than what is known [5]), to construct a lattice structure that will give the energy efficient encoding, eventually looking at non maximal orders of the number field, and finally to make sure to have a division algebra.

Finally, though the optimality of the Golden Code was shown inside the class of cyclic division algebras, there is

no construction using other methods known to do better than the Golden Code.

## ACKNOWLEDGMENTS

The author would like to thank Prof. E. Viterbo for his careful reading of this note, and Dr. J. Lahtonen for sending a preprint of his work.

## REFERENCES

- [1] J.-C. Belfiore, G. Rekaya, E. Viterbo, "The Golden Code: A 2 x 2 Full-Rate Space-Time Code with Non-Vanishing Determinants," *IEEE Transactions on Information Theory*, vol. 51, n. 4, pp. 1432-1436, April 2005.
- [2] P. Dayal, M.K. Varanasi, "An Optimal Two Transmit Antenna Space-Time Code and its Stacked Extensions," *Proceedings of Asilomar Conf. on Signals, Systems and Computers*, Monterey, November 2003.
- [3] P. Elia, B. A. Sethuraman and P. Vijay Kumar, "Perfect Space-Time Codes with Minimum and Non-Minimum Delay for Any Number of Antennas," *Proc. WirelessCom 2005*, International Conference on Wireless Networks, Communications, and Mobile Computing.
- [4] C. Hollanti, J. Lahtonen, K. Ranto and R. Vehkalahti, "Optimal Matrix Lattices for MIMO Codes from Division Algebras", in the proceedings of *ISIT 2006*, Seattle.
- [5] F. Oggier, G. Rekaya, J.-C. Belfiore, E. Viterbo, "Perfect Space-Time Block Codes," *IEEE Trans. Inform. Theory*, vol. 52, n.9, September 2006.
- [6] F. Oggier, G. Berhuy, "On Improving 4 x 4 Space-Time Codes", to appear in the proceedings of *Asilomar conference 2006*.
- [7] B. A. Sethuraman, B. S. Rajan, and V. Shashidhar, "Full-diversity, high-rate space-time block codes from division algebras," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2596- 2616, October 2003.
- [8] V. Tarokh, N. Seshadri, and A. Calderbank, "Space-time codes for high data rate wireless communication : Performance criterion and code construction," *IEEE Trans. Inform. Theory*, vol. 44, pp. 744-765, March 1998.
- [9] H. Yao, G.W. Wornell, "Achieving the Full MIMO Diversity-Multiplexing Frontier with Rotation-Based Space-Time Codes," *Proceedings of Allerton Conf. on Communication, Control and Computing*, October 2003.
- [10] L. Zheng, D. Tse, "Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels," *IEEE Trans. on Information Theory*, vol. 49, no. 5, pp. 1073-1096, May 2003.